Using Entropy Tokens with FortiGate Products

Technical Note

Using Entropy Tokens with FortiGate Products Technical Note

March 5, 2015

Revision 1

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Using Entropy Tokens with FortiGate Products

Fortinet currently uses the Araneus Alea II TRNG as an entropy source for FIPS 140-2 and Common Criteria NDPP compliance. The Alea II TRNG is a hardware entropy source USB token for use with Fortinet products. Based on a wide-band Gaussian white noise generator, the entropy token provides you with a simple source of entropy.

The Alea II is available directly from Araneus. Visit the Araneus website for pricing and ordering information:

https://ssl.araneus.fi/products/alea2/order/en/

Supported firmware versions

The entropy token is supported by FortiOS 5.0.10 or later.

FIPS 140-2 and Common Criteria Certified firmware/software

Fortinet certifies specific firmware images and software releases for FIPS 140-2 and Common Criteria. Refer to the support site product download directories for details on which firmware/software versions are certified or contact your sales representative for more information.

Supported hardware models

The entropy token requires a USB-A port. All hardware supported by FortiOS 5.0.10 or later support the entropy token except for models that do not have a USB-A port. Models that do not have a USB-A port are listed below.

- FortiGate
  - FortiGate 60C-PoE

Configuration

The entropy token is enabled by default when the FIPS-CC mode of operation is enabled. To enable FIPS-CC mode, enter the following Command Line Interface (CLI) commands and follow the instructions:

```
config system fips-cc
    set status enable
end
```

Enabling the entropy token in default mode

The entropy token can also be used in the default mode of operation (non-FIPS-CC mode) with the following CLI commands:

```
config system fips-cc
   set entropy-token <enable/disable/dynamic>
end
```

Entropy token settings

There are three settings available for the entropy token:

enable — the token is required.

disable — the token is not used even if present.

dynamic — the token is not required, but is used if present.

For example, to enable FIPS-CC mode and disable use of the token, enter the following CLI commands:

```
config system fips-cc
  set entropy-token disable
  set status enable
end
```

Additional information

Once the entropy token is enabled, it is used to seed the product's internal Random Number Generator (RNG). The RNG is seeded during the boot process and then reseeded periodically. The default reseed period is once every 24 hours (1440 minutes). The reseed interval can be configured using the following CLI commands:

```
config system fips-cc
  set self-test-period <1-1440 minutes>
end
```

The self-test-period setting is only available in the FIPS-CC mode of operation.

The entropy token must be present to allow the RNG to seed or reseed from the token.

When FortiOS is configured in FIPS-CC mode with the entropy token enabled, if the token is not present at boot time, the boot process will pause until the token is inserted. The following message is displayed on the console:

"Please insert entropy-token to complete RNG seeding"

The message is repeated until the token is inserted. If the token is not present at the reseed interval, the same message is also repeated until the token is inserted.

If the entropy token is set to dynamic and the token is not present at boot time or the scheduled reseed interval, the appliance will use the default, internal FortiOS seed method instead.